In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct

DENNIS D. HIRSCH*

TABLE OF CONTENTS

* Geraldine W. Howell Professor of Law, Capital University Law School. The author would like to thank Professor Peter Swire who organized the Law Journal Symposium in which this paper was first presented, the other participants in the Symposium, the editors of the *Ohio State Law Journal*, Capital University Law School which provided the summer research grant that made possible the writing of this Article, and Natalia Messenger for her valuable research assistance.

I. INTRODUCTION

The movement of personal data across national borders is fundamental to the Internet economy.[1] Yet the laws that govern such data flows remain national or, at best, regional.[2] This mismatch creates a number of related problems. It makes it difficult to track and enforce compliance as personal data moves rapidly and unpredictably from one legal jurisdiction to another.[3] It increases costs and risks for businesses that must track, and seek to comply with, a wide variety of privacy laws.[4] And it creates tension and political strife between major trading partners, such as the United States and the European Union (E.U.), whose differing approaches to privacy law threaten to disrupt data transfers across their borders.[5] The Department of Commerce has identified the conflict between global data flows and national or regional laws as one of the most significant problems facing privacy law and policy today, explaining that "[d]isparate approaches to commercial data privacy can create barriers to both trade and commerce, harming both consumers and companies."[6]

There may be a relatively simple and elegant solution to this problem: internationally approved, industry codes of conduct. The solution would work as follows. An industry sector would draft a privacy code of conduct that fulfilled the core requirements of the E.U.'s 1995 Data Protection Directive, the Asia-Pacific Economic Cooperation (APEC) forum's Privacy Principles and, perhaps, other regional privacy regimes. It would then submit the code to the relevant authority in each such regional jurisdiction. If the authority approved the code, firms that complied with it would know that their activities met the legal requirements for that jurisdiction (the E.U., the APEC nations, etc.). A single industry code of conduct, approved in each of these regional jurisdictions, would be able to function as a nearly global set of privacy rules for that sector.

This Article is not alone in looking to industry codes of conduct as a potential solution to the privacy problems associated with international data

---

[1] *See generally* PAUL M. SCHWARTZ, THE PRIVACY PROJECTS, MANAGING GLOBAL DATA PRIVACY: CROSS-BORDER INFORMATION FLOWS IN A NETWORKED ENVIRONMENT (2009) (describing commercial data transfers across national borders).

[2] *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1336–39 (2000) (describing the conflict between international data flows and national laws).

[3] *See infra* notes 55–62 and accompanying text.

[4] *See infra* notes 63–72 and accompanying text.

[5] *See infra* notes 68–70 and accompanying text.

[6] INTERNET POLICY TASK FORCE, DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC FRAMEWORK 53 (2010) [hereinafter DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY].

flows. Policymakers in Europe, Asia and the United States have also been using industry codes to address this issue: The E.U. through its Binding Corporate Rules (BCR) initiative; the APEC forum through its Cross-border Privacy Rules program; and the United States and E.U. through their Safe Harbor Agreement.[7] Each of these important initiatives employs codes of conduct as a means to create cross-border privacy rules.[8]

This Article's approach differs from these existing initiatives in a critical way. Each of the programs just named uses codes of conduct created at the level of the *individual firm*, rather than at the level of the industry sector. This weakens these efforts. It renders the code of conduct approach impractical for most companies, expensive for governments to administer and enforce, and difficult for stakeholder groups to track and monitor. This Article identifies an alternative approach—*sector-based* codes of conduct (i.e., codes created at the level of the industry sector)—and explains why it avoids the problems just mentioned and holds the most promise going forward. It then identifies the legal reforms needed to make this approach work.

Part II of the Article describes the huge growth in international data flows, the ways in which they conflict with national and regional privacy laws, and the challenges that this creates for privacy protection, commerce, and international relations. Part III draws on regulatory theory to assess whether direct government regulation (i.e., treaties implemented through national law), pure industry self-regulation, or enforceable codes of conduct are best suited to address this problem. In so doing, it sheds light on the advantages of the code of conduct approach and why policymakers and industry have become so focused on it. Part IV evaluates the existing code of conduct initiatives—Binding Corporate Rules, APEC Cross-border Privacy Rules, and the U.S.–E.U. Safe Harbor Agreement. It explains that each of these initiatives focuses on firm-based codes of conduct (i.e., codes negotiated at the level of the individual firm), and that this reduces their effectiveness. It argues that sector-based, cross-border codes of conduct would work much better. Part V analyzes whether existing legal mechanisms can support cross-border, sector-based codes of conduct. It shows that many of the necessary pieces are already in place. It identifies the legal reforms that will be needed to make this approach work.

II. GLOBAL DATA FLOWS, NATIONAL PRIVACY LAWS, AND THE PROBLEMS THEY CREATE FOR ONE ANOTHER

Technology leaps forward and changes social realities. The law evolves slowly to address these new challenges. For a time, there is a mismatch between technology and society on the one hand, and law on the other. Eventually, the

---

[7] *See infra* Parts IV.A, IV.B, IV.C.

[8] *See infra* Parts IV.A, IV.B, IV.C.

law adapts to the new realities. This is an old story, repeated in many contexts.[9] The rise of global data flows, and their conflict with slow-changing national and regional privacy laws, is this story on steroids. The establishment of the Internet, and the consequent increase in cross-border data transfers, has been dizzying in its speed, size and complexity. The disjunction between this rapidly expanding global data network, and the national and regional laws that seek to govern it, is profound and problematic.

A. *Global Data Flows*

The World Wide Web (www) is just that. It creates a global architecture for the transfer of digital data that does not respect national or regional boundaries.[10] It should not be surprising, then, that the emergence of the Internet and, subsequently, the Cloud,[11] have exponentially increased the speed, and decreased the cost, of cross-border transfers of personal data. As Professor Paul Schwartz has explained, this has led to three, related changes in data processing.[12]

First, it has increasingly made data processing into a cross-border affair. Prior to the rise of the Internet, most data processing data took place within the boundaries of a single nation.[13] The transfer of data across national borders was "an occasional event, an exception and not the rule."[14] Today, cross-border data transfers are ubiquitous.[15] The low cost of international data transfer has allowed companies to locate operations, and develop relationships with other businesses and customers, throughout the world.[16] They then collect personal data from, and/or share data with, each of these individuals or entities.[17] International data transfers and economic globalization build on and reinforce one another. Fast, cheap, and reliable international data transfers support the

---

[9] *See* Dennis D. Hirsch, *Introduction: The Information Economy, the War on Terror and the Evolving Landscape of Information Privacy Law*, 5 ISJLP 409, 409–12 (2010) [hereinafter Hirsch, *Information Economy*] (describing this process in a number of areas of law).

[10] Reidenberg, *supra* note 2, at 1322–23 ("[T]he entire architecture of the Internet is based on the principle of geographic indeterminacy. . . . Data may be collected in one location, processed elsewhere, and stored at yet another site.").

[11] Cloud computing is "the location of computing resources on the Internet in a fashion that makes them highly dynamic and scalable." SCHWARTZ, *supra* note 1, at 5.

[12] *Id.* at 8.

[13] *Id.* at 5, 10.

[14] *Id.*

[15] Reidenberg, *supra* note 2, at 1316–17; *see also* DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY, *supra* note 6, at 19 ("Unlike traditional mass media, the Internet is global.").

[16] SCHWARTZ, *supra* note 1, at 17 (IT revolution facilitated globalization).

[17] *Id.* at 20 (explaining data transfers based on process optimization, not physical proximity).

growth of global business.[18] Increased economic globalization, in turn, widens the demand for, and investment in, rapid and inexpensive cross-border data transfers.[19] The upshot is an "exponentially increased . . . flow of personal information across national borders."[20]

The second important change has been the rise in data processing networks. Previously, most companies employed localized, central databases. Insofar as they transmitted data across borders, they sent it from one centralized database to another.[21] These were point-to-point transactions between two discrete databases. Today, many businesses participate in multi-point data processing networks.[22] An example would be a multinational company that utilizes a third-party vendor for its personnel recruitment.[23] Company offices located around the world send job postings to the vendor.[24] Recruitment agencies, individual applicants, and current employees (making recommendations) located in many different countries send applications and other personal information to the vendor, which shares it with the human resources departments at the multinational firm's various locations.[25] Company human resources departments may request additional information, leading to another round of multi-point data transfers.[26] This network of data flows involves many different entities, located in different countries, in a complex stream of data transfers.[27] Such networks, which are increasingly common today, result in a nearly constant flow of personal information across national borders[28] and have resulted in "a massive growth in the complexity and volume of these transfers."[29] Nothing like this was possible prior to the Internet.

The third change is the shift from discrete, one-time data transmissions, to far more dynamic, ongoing transfers of personal information. In an earlier era, a company would prepare for an international transfer of personal data and then implement it at a single, pre-defined point in time.[30] These were "static"[31]

---

[18] *See, e.g.*, Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 AM. BUS. L.J. 413, 418 (2013) (describing the benefit for companies using Cloud).

[19] Reidenberg, *supra* note 2, at 1317.

[20] *Id.*

[21] SCHWARTZ, *supra* note 1, at 17 ("[D]ata [goes] from one established database to another."). An example would be a subsidiary that transferred human resources data from its own local database, to that of its parent company. *Id.* at 11 (providing such an example).

[22] *See id.* at 8.

[23] *Id.* at 15.

[24] *See id.*

[25] *Id.* at 23.

[26] *See id.* at 15.

[27] *See* SCHWARTZ, *supra* note 1, at 15.

[28] *Id.* at 8.

[29] *Id.*

[30] *Id.* at 16.

[31] *Id.* at 5.

events in the sense that they took place, and then they ended. Currently, cross-border data transfers take place on demand, continuously, and in real time.[32] They are "dynamic"[33] in the sense that they can occur at any given moment, have no discrete ending point, and are often difficult if not impossible to predict in advance.[34] An example would be a technology company that has set up support centers in India, Costa Rica, and Bucharest. When a customer contacts the company, the firm uses an algorithm based on factors such as time of day and customer location, to determine which service location should handle the contact.[35] It then gives that center access to the customer's personal information and directs the customer to it.[36] The result is an international flow of personal data relating to customer service calls that is context-dependent, "extremely dynamic and cannot necessarily be predicted in advance."[37]

In sum, the rise of the Internet has "exponentially increased" the volume of international transfers of personal data.[38] It has also changed the nature of these transmissions from transfers that were generally local, point-to-point, and discrete, into global data flows that are increasingly cross-border, networked, multi-point, continuous, and dynamic.[39]

B. *The Conflict Between Global Data Flows and National Data Protection Laws*

Democratic nations broadly agree on the core privacy protections that should apply in the commercial sphere.[40] The Organization for Economic Co-operation and Development's (OECD) widely endorsed list of Privacy Principles is the best reflection of this consensus.[41]

---

[32] *Id.* ("Modern information systems respond to data requests rapidly and in many instances in real time."); *id.* at 8.

[33] SCHWARTZ, *supra* note 1, at 13.

[34] *Id.* at 22.

[35] *Id.* at 14.

[36] *Id.*

[37] *Id.* at 22.

[38] Reidenberg, *supra* note 2, at 1317; *see also* SCHWARTZ, *supra* note 1, at 8 ("There has been a massive growth in the complexity and volume of [international data] transfers."); Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071 (2013).

[39] Professor Schwartz provides another example that nicely captures this set of developments. A marketing firm in Spain obtains a list of potential customers from a global Customer Relationship Management (CRM) system in the United States. SCHWARTZ, *supra* note 1, at 13. It shares this list with its call center in Mexico, which uses it to execute a telemarketing campaign in Spain. *Id.* The Spanish marketing company then shares the results of its telemarketing effort with the U.S. vendor, which uses it to update the information in its global CRM system. *Id.*

[40] Reidenberg, *supra* note 2, at 1325.

[41] *See* Ben Gerber, *The Privacy Principles*, OECD PRIVACY, http://oecdprivacy.org/#principles (last visited Oct. 5, 2013) (listing the OECD Privacy Principles).

The important differences among national systems occur, not with respect to these broad principles, but in how countries interpret and apply them.[42] Examples abound. Some nations define "personally identifiable information" (PII) more broadly than others.[43] Some exclude certain types of personal information, even if it falls within the definition of PII.[44] Countries disagree on what constitutes adequate notice.[45] As a result, "data collectors [may not be able to] use the same notice for residents of different jurisdictions."[46] Nations differ on what counts as meaningful choice, and as to when choice must be opt-in and when it can be opt-out. The European Union requires companies to notify the data subject of their data collection activities, and the data protection authorities of their data processing operations.[47] The United States does not.[48] E.U. nations have omnibus privacy laws.[49] Others, such as the United States, use sectoral laws.[50] Nations also differ significantly in the execution and enforcement of their divergent privacy laws.[51] Some provide more oversight and enforcement; some less.[52] Some have active data protection authorities (DPAs); some more passive DPAs; and some, such as the United States, have no DPA at all.[53]

These differences are particularly salient on the Internet where personal data are more likely to travel among a variety of legal jurisdictions and where these "[i]nternational data flows . . . [force] divergent data protection policies and rules to confront each other with ever greater frequency."[54] They cause major difficulties for governments and individuals who wish to protect personal information as it travels across the globe, and for businesses that depend on the cross-border transfer of personal data.

---

[42] Reidenberg, *supra* note 2, at 1330–35.

[43] *Id.* at 1333.

[44] *See id.*

[45] *See id.* at 1338.

[46] *Id.*

[47] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, arts. 10, 11, 18, 1995 O.J. (L 281) 31 (EC) [hereinafter 1995 Directive].

[48] Reidenberg, *supra* note 2, at 1334 ("U.S. law does not generally impose an obligation to inform individuals that data about them is being collected.").

[49] *Id.* at 1330.

[50] *Id.* at 1331.

[51] *Id.* at 1330.

[52] *Id.* at 1334–35.

[53] *Id.* at 1345 ("There is no data protection commission in the United States.").

[54] Reidenberg, *supra* note 2, at 1318; *see also id.* at 1336 ("The Internet places divergent rules in proximity through architectural features that promote geographic indeterminacy."); Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 472, 486–87 (1995) (transferring data between United States and Europe faces significant challenges).

1. *Problems for Privacy Protection*

The differences among national privacy regimes, combined with the explosion in global data transfers, pose a fundamental challenge for the protection of individual privacy. At the most basic level, a processor may move a person's data from a jurisdiction with stringent and well-enforced privacy laws, to one with lenient and poorly enforced rules.[55] Some companies may purposely operate this way in order to take advantage of "regulatory arbitrage."[56] Global data flows, combined with national privacy laws, can accordingly result in the migration of personal data to those nations with the weakest laws or, at minimum, to temporary gaps in privacy protection as the data moves through such a jurisdiction.[57]

Even where each of the relevant nations has implemented meaningful privacy laws, the cross-border nature of today's data transfers makes it difficult to track compliance with them. For example, the dynamism and unpredictability of global data flows make it difficult to tell where personal data is at any given moment, which entity is responsible for it,[58] or which jurisdiction's laws apply.[59] This difficulty in establishing clear jurisdiction can, in turn, inhibit enforcement[60] and make it hard for individuals to seek remedies for violations.[61] The overall effect is to create "uncertainty and instability of the protection of individuals['] [privacy]."[62]

2. *Problems for Business*

The lack of consistency among national laws also creates significant problems for the businesses that engage in cross-border transfers of personal data and desire to comply with legal requirements.[63] These companies must

---

[55] Reidenberg, *supra* note 2, at 1337 (stating that some jurisdictions have far weaker information privacy rules than others).

[56] *Id.* at 1332.

[57] DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY, *supra* note 6, at 54 (explaining differing national privacy laws can lead to "gaps in protection for consumers whose data are transferred across borders, since it is not always clear who has jurisdiction over data and what protections exist for foreign consumers").

[58] Reidenberg, *supra* note 2, at 1323 (stating when multiple entities interact with data this can "obscure the responsibility for data protection").

[59] *Id.* at 1336 (explaining that multiple nations may assert jurisdiction over a networked set of data transfers).

[60] *Id.* at 1336 n.114 (citing Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1216–21 (1998)).

[61] Sunni Yuen, *Exporting Trust with Data: Audited Self-regulation as a Solution to Cross-border Data Transfer Protection Concerns in the Offshore Outsourcing Industry*, 9 COLUM. SCI. & TECH. L. REV. 41, 44 (2008).

[62] Reidenberg, *supra* note 2, at 1351.

[63] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL

closely track the flow of their data in order to know which jurisdiction's rules apply at any given moment. They must understand and monitor compliance with the privacy laws of each jurisdiction through which their data travels. Finally, they may need to seek multiple regulatory approvals for routine, cross-border data transfers.[64] These tasks make it far more costly and burdensome to achieve compliance than it would be if companies were able to follow a single set of privacy rules throughout their data's lifecycle.[65] As the Department of Commerce has recognized, companies face "difficulties in complying with the multiplicity of foreign data protection rules and regulations."[66]

Differing privacy laws also confront businesses with uncertainty. The dynamism of global data flows makes it difficult for companies to predict where, and at what time, they will transfer data across borders and so to comply with the relevant laws. In addition, conflicts between nations and/or regions with respect to the adequacy of their respective privacy laws can raise the prospect of data embargoes.[67] The European Union considers U.S. privacy law inadequate and may limit data transfers to the United States,[68] although the relevant governments have managed to avoid this so far by means of the Safe Harbor Agreement and other understandings.[69] Still, the prospect of a data embargo creates profound uncertainty for businesses that depend on the free flow of personal data across national borders.[70] Such uncertainty can drive up the cost of capital, inhibit investment and innovation, and cause tension between international allies.

The difficulties that consumers face, and those that businesses confront, reinforce and build on one another. When consumers lose faith in the law's ability to protect their personal information, this can cause them to pull back from online businesses. This can, in turn, hurt the companies whose business models depend on a certain level of consumer trust and participation in the

---

DIGITAL ECONOMY 31 (2012) ("Differences in national privacy laws create challenges for companies wishing to transfer personal data across national borders."); *see* Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1254–57 (2013).

[64] THE WHITE HOUSE, *supra* note 63, at 31 ("Complying with different privacy laws is burdensome for companies that transfer personal data . . . because legal standards may vary among jurisdictions, and companies may need to obtain multiple regulatory approvals to conduct even routine operations.").

[65] DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY, *supra* note 6, at 14 ("[T]he lack of cross-border interoperability in privacy principles and regulations creates barriers to cross-border data flow and significant compliance costs for companies.").

[66] *Id.* at 53–54.

[67] *See id.*

[68] *See* Reidenberg, *supra* note 2, at 1337–38. *See generally* Bartosz M. Marcinkowski, *Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard*, 74 OHIO ST. L.J. 1167 (2013).

[69] *See infra* Part IV.C.

[70] *See* Reidenberg, *supra* note 2, at 1351.

Internet economy.[71] By the same token, companies that face increased compliance costs and uncertainties are likely to pass these costs on to consumers, insofar as they can. This can lead to higher prices for the goods and services that consumers would like to purchase. The failure to harmonize national privacy laws can accordingly result in higher prices for consumers.[72]

For all of the above reasons, the jumble of inconsistent national and regional privacy laws conflicts with the contemporary trend towards increasingly global data flows and poses a challenge to the continued growth and vibrancy of the Internet and of the global economy.[73] The emergence of a unified set of privacy rules, on the other hand, would diffuse this threat and provide benefits to both consumers and industry.[74] The Department of Commerce has called for "a new global framework for privacy protection that will decrease the cost of doing business globally, provide consumers with consistent levels of protection worldwide, and contribute to global economic growth."[75] The question is: how to achieve this?

III. REGULATORY OPTIONS

This is a question of regulatory design. It is accordingly important to begin by consulting regulatory theory with respect to the possible approaches.

Any question of regulatory design requires the designer to answer two basic questions. First, who will regulate? Second, at what level will that entity regulate? The first question—who will regulate?—has three possible answers:[76]

---

[71] DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY, *supra* note 6, at 15 (stating that the maintenance of "consumer trust is vital to the success of the digital economy"); Reidenberg, *supra* note 2, at 1351 ("The uncertainty and instability of the protection of individuals will be harmful to international data flows and the wider development of a robust online community.").

[72] *See* DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY, *supra* note 6, at 56.

[73] *Id.* at 14 ("Improving the global interoperability of data privacy approaches could enable increased exports of U.S. services and strengthen the American economy."); THE WHITE HOUSE, *supra* note 63, at 31 ("[I]t is critical to the continued growth of the digital economy that [governments] strive to create interoperability between privacy regimes.").

[74] DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY, *supra* note 6, at 56 ("[M]utual recognition of substantively similar commercial data privacy laws around the world can build increased practical protection for consumers and reduce barriers and compliance costs for business.").

[75] *Id.* at 57.

[76] CHRISTOPHER T. MARSDEN, INTERNET CO-REGULATION: EUROPEAN LAW, REGULATORY GOVERNANCE AND LEGITIMACY IN CYBERSPACE 51–58 (2011) (distinguishing between government regulation, self-regulation, and co-regulation); *see also* HANS-BREDOW-INSTITUT, FINAL REPORT: STUDY ON CO-REGULATION MEASURES IN THE MEDIA SECTOR 17 (2006); Neil Gunningham & Joseph Rees, *Industry Self-regulation: An Institutional Perspective*, 19 L. & POL'Y 363, 365–66 (1997); Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-regulation, or Co-regulation?*, 34 SEATTLE U. L. REV. 439, 465 (2011) [hereinafter Hirsch, *Online Privacy*]; BERT-JAAP KOOPS ET AL., *Should Self-regulation Be the Starting Point?*, *in* STARTING POINT FOR ITC REGULATION:

(1) government will regulate industry (direct government regulation),[77] (2) industry will regulate itself (self-regulation),[78] and (3) government and industry will intentionally and expressly *share* responsibility for the drafting and enforcement of rules ("co-regulation").[79] The second question—at what level will that entity regulate?—likewise has three possible answers: (1) regulate at the level of the individual company (company-based regulation), (2) regulate at the level of the industry sector (sector-based regulation), or (3) regulate at the level of the economy as a whole (economy-wide regulation).[80] These two questions, and their respective possible answers, yield nine possible regulatory design combinations as reflected in the following table.

Table 1: *Regulatory Design Options*

	Direct Government Regulation	*Self-regulation*	*Co-regulation*
Company	1	4	7
Sector	2	5	8
Economy as a Whole	3	6	9

Governments could use any of these nine options to create international privacy rules. The remainder of this Section will evaluate which of these regulatory options is best suited to this task.

DECONSTRUCTING PREVALENT POLICY ONE-LINERS 109, 119–23 (Bert-Jaap Koops et al. eds., 2006); Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 355, 357–58 (2011).

[77] MARSDEN, *supra* note 76, at 54; *see also* Gunningham & Rees, *supra* note 76, at 366; Margot Priest, *The Privatization of Regulation: Five Models of Self-regulation*, 29 OTTAWA L. REV. 233, 237–38 (1997–1998).

[78] Gunningham & Rees, *supra* note 76, at 365; Priest, *supra* note 77, at 238 (describing "entirely voluntary systems of regulation").

[79] MARSDEN, *supra* note 76, at 46; Gunningham & Rees, *supra* note 76, at 366; Rubinstein, *supra* note 76, at 357. In some sense, most regulation could be said to be co-regulatory. Government frequently consults industry—either through notice-and-comment rulemaking, or more informally—when it engages in direct regulation. *See* Gunningham & Rees, *supra* note 76, at 366. By the same token, industry often looks to government for input and feedback when it engages in self-regulation. *See* MARSDEN, *supra* note 76, at 63 ("Pure self-regulation with no prior or later approval amounts to a self-regulatory body that is close to invisible in practice."). To demarcate co-regulation, it helps to think of a continuum with pure industry self-regulation on one end (i.e., no government involvement), and pure government regulation on the other (i.e., no industry role). *See* Gunningham & Rees, *supra* note 76, at 366 (describing a "continuum, with pure forms of self-regulation and government regulation at opposite ends"). Co-regulation encompasses those initiatives that stand towards the middle of this continuum—the programs in which government and industry intentionally and expressly combine their efforts and collaborate on the production, monitoring and enforcement of rules. *See id.*

[80] *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 155 (2006) (distinguishing between "organizational" and "sectoral" codes); Gunningham & Rees, *supra* note 76, at 365.

A. *Direct Government Regulation*

In direct regulation, government officials create, monitor compliance with, and enforce the regulatory requirements.[81] To establish cross-border privacy rules through direct regulation, participating countries would first adopt a treaty or convention establishing international privacy requirements. Each ratifying nation would then promulgate national laws and regulations that closely tracked the international template and would enforce these requirements against companies in their jurisdiction. In such a way, direct, government regulation would establish uniform, cross-border privacy rules. Professor Joel Reidenberg has called for an "international treaty on data protection" along these lines.[82]

The strengths of such an approach would be those commonly associated with direct regulation. Governments would likely establish relatively uniform, socially protective sets of rules. The uniformity would make it easier for regulators to monitor compliance with, and to enforce, these rules.[83] It would also create a level playing field for business.[84]

Direct regulation, in the form of national laws enforcing an international treaty, would also face important obstacles and present significant downsides. The first obstacle is a practical one; it is extremely difficult to establish an international treaty of any sort.[85] This task becomes even harder when the treaty in question would address an issue, such as privacy, as to which there are deep cultural and regional differences.[86] It is one thing to set out a broad set of privacy principles, as the OECD has done, and get a variety of nations to sign on to them. It is quite another to negotiate a detailed treaty establishing concrete privacy requirements and convince countries to ratify, implement, and enforce them. Practical difficulty is one of the major downsides of a direct regulation approach. It may explain why there have been no serious attempts to create such a treaty.

Even if it were possible to impose cross-border privacy rules through direct regulation, regulatory theory suggests that this may not be the optimal approach for this particular area. Direct government regulation works better in some

---

[81] Priest, *supra* note 77, at 238; *see also* MARSDEN, *supra* note 76, at 54.

[82] Reidenberg, *supra* note 2, at 1360. Professor Reidenberg suggests following the model of the General Agreement on Tariffs and Trade (GATT) and creating a "General Agreement on Information Privacy (GAIP)." *Id.* (internal quotation marks omitted).

[83] *See* JAMES SALZMAN & BARTON H. THOMPSON, JR., ENVIRONMENTAL LAW AND POLICY 49 (2003).

[84] *See* Howard Latin, *Ideal Versus Real Regulatory Efficiency: Implementation of Uniform Standards and "Fine-Tuning" Regulatory Reforms*, 37 STAN. L. REV. 1267, 1271 (1985).

[85] *See* VIRGINIA HAUFLER, A PUBLIC ROLE FOR THE PRIVATE SECTOR: INDUSTRY SELF-REGULATION IN A GLOBAL ECONOMY 115 (2001) (explaining that negotiating binding international agreements is "difficult, defensive, and often leads to inflexible rules").

[86] *See id.* at 82 (discussing difficulty of direct, top-down regulation due to lack of consensus on the "mechanisms and standards for international privacy protection").

contexts than in others.[87] It can do a good job of regulating slower-moving areas of the economy that pose significant risks to the public.[88] The regulation of toxic pollutants from manufacturing operations would be one such example.[89] However, direct government regulation is not well-suited to areas, such as privacy regulation, where the technologies and business models change rapidly and continuously.[90] In these situations, it is difficult for government officials to know enough about the industries in question to craft intelligent rules that account for business realities. Moreover, government regulation's lengthy time frame (e.g., notice-and-comment rulemaking) often fails to keep pace with fast-moving technological and business changes.[91] Business realities end up "lapping" the government rules intended to regulate them, rendering these rules out-of-date or even obsolete.

B. *Self-regulation*

It is for these reasons that some question the viability of direct government regulation and consider self-regulation to be the best approach to privacy governance.[92] Under this approach, industry sets, monitors, and enforces its own standards.[93] Multinational companies could use self-regulation to set uniform, cross-border privacy rules. To do so a specific company, or a sector organization that represents it, could establish a voluntary set of privacy rules. The company would then commit to following that set of rules throughout its international operations and so establish a single, global set of privacy rules for the company.

Proponents of self-regulation argue that, since it comes from industry itself, it is able to tap into business knowledge and is thereby able to produce more

---

[87] *See* Neil Gunningham, *Environmental Management Systems and Community Participation: Rethinking Chemical Industry Regulation*, 16 UCLA J. ENVTL. L. & POL'Y 319, 327 (1998).

[88] *Id.*

[89] Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 34 (2006) [hereinafter Hirsch, *Inner Environment*].

[90] Gunningham, *supra* note 87, at 327; Hirsch, *Inner Environment*, *supra* note 89, at 35; *see also* HAUFLER, *supra* note 85, at 115 (concluding that binding international agreements can lead to "inflexible rules that do not achieve their aims").

[91] Hirsch, *Inner Environment*, *supra* note 89, at 35; *see* OFFICE OF TECH. ASSESSMENT, U.S. CONG., ENVIRONMENTAL POLICY TOOLS: A USER'S GUIDE 27–28 (1995); Richard B. Stewart, *A New Generation of Environmental Regulation?*, 29 CAP. U. L. REV. 21, 31 (2001).

[92] HAUFLER, *supra* note 85, at 92 (discussing those who believe that government should not seek to regulate information privacy, and should leave the task to industry self-regulation, because "government regulators" are not capable of dealing with the "rapid changes and complex issues of the new information economy").

[93] Priest, *supra* note 77, at 256; *see* Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897, 910–12 (2013).

intelligent and effective rules than government regulation.[94] They further argue that self-regulatory entities, which do not need to comply with notice-and-comment procedures and other legal requirements, should be able to update their rules far more quickly than government regulators can.[95] Self-regulation should therefore do a better job of keeping pace with rapidly evolving technological and business realities. Finally, proponents of self-regulation maintain that companies, which often resist government-imposed rules, will be more likely to accept rules that they or their peers have drafted.[96] Self-regulation will accordingly promote greater industry buy-in and compliance.

Notwithstanding the proponents' arguments, there are both practical and theoretical reasons to doubt that self-regulation is the best choice for international privacy rules. To begin with, self-regulation, by definition, does not involve formal government approval.[97] As a consequence, it neither provides the legal safe harbor that companies need to engage confidently in cross-border data transfers, nor absolves firms from the costly duty of having to track and comply with multiple national privacy laws. It does not truly address the mismatch between global data flows and national data protection laws and so will not achieve the practical goals that motivate the search for global privacy rules in the first place.

Regulatory theory suggests additional reasons to be cautious about self-regulation. Businesses have an incentive to draft self-regulatory rules that appear to offer solid protection but are not, in fact, very stringent.[98] Self-regulation accordingly tends to be more lenient than government requirements, and may not achieve public goals like privacy.[99] Theory further predicts that companies may commit to impressive-sounding self-regulatory goals but then fail to subject themselves to the independent monitoring needed to make these claims credible.[100]

---

[94] *See* KOOPS ET AL., *supra* note 76, at 109 (discussing those who take this position); *see also* Gunningham & Rees, *supra* note 76, at 366.

[95] Gunningham & Rees, *supra* note 76, at 366 (discussing those who take this position); *see also* Jared Strauss & Kenneth S. Rogerson, *Policies for Online Privacy in the United States and the European Union*, 19 TELEMATICS & INFORMATICS 173, 181 (2002).

[96] *See* Gunningham & Rees, *supra* note 76, at 366.

[97] Priest, *supra* note 77, at 238.

[98] *See* BENNETT & RAAB, *supra* note 80, at 154 (stating that company privacy commitments tend to be more "public relations" than substance); *cf.* Rhys Jenkins, *Corporate Codes of Conduct: Self Regulation in a Global Economy*, UNITED NATIONS INST. FOR SOC. DEV. PROGRAMME ON TECH. BUS. & SOC'Y, Apr. 2001, at 28, *available at* http://www.unrisd.org/unrisd/website/document.nsf/%28httpPublications%29/E3B3E78BA B9A886F80256B5E00344278?OpenDocument (explaining that self-regulation generally focuses on issues that are damaging to a company's reputation but does not address other important issues).

[99] *See* BENNETT & RAAB, *supra* note 80, at 134.

[100] Jenkins, *supra* note 98, at 27; KOOPS ET AL., *supra* note 76, at 137; Strauss & Rogerson, *supra* note 95, at 183.

International privacy self-regulation exists at the company and economy-wide levels. Multinational corporations have established corporate privacy policies and required each of their units to comply with them.[101] This is a form of cross-border privacy self-regulation at the level of the individual company. The International Commerce Exchange (ICX) drafted an economy-wide privacy standard that any company could adopt.[102] ICX believed that its standard would ensure "adequate" protection under the E.U.'s 1995 Data Protection Directive and so allow companies that followed it to engage in cross-border data transfers.[103]

Can international self-regulatory codes provide a harmonized set of rules that will allow companies to achieve compliance across national borders? There are reasons to doubt that they can serve this function. To begin with, as described above, governments do not review or approve self-regulatory requirements. As a result, companies that follow these rules cannot be sure that they are in compliance with the laws of the nations among which they transfer data. Such firms still have to spend resources on learning and meeting many different sets of national and regional privacy requirements. Compliance with a self-regulatory standard does not reduce this burden and so provides companies with little incentive to sign up for and comply with such a standard.

The ICX code of conduct illustrates this. ICX hoped to convince the European Commission that the code constituted "adequate" protection for the purposes of the Directive and to have the Commission approve it.[104] With such approval in hand, companies from any economic sector of the economy that complied with the code would have been able to transfer E.U. citizens' personal information to any location in the world without running afoul of the adequacy requirement.[105] However, ICX was not able to obtain European approval of its draft code and so could not guarantee international compliance to companies that adopted it.[106] Few firms committed to follow the ICX code and few today have even heard of it. This suggests that, without the ability to guarantee legal compliance, pure self-regulation will neither attract sufficient industry involvement nor address the need for international privacy standards.

---

[101] *See* BENNETT & RAAB, *supra* note 80, at 155 (stating multinational corporations adopt privacy policies); HAUFLER, *supra* note 85, at 22 (maintaining multinationals adopt global corporate policies "so that they would not have to deal with such a welter of conflicting national regulatory systems"); Jenkins, *supra* note 98, at 23 (declaring multinational corporations adopt social responsibility policies in order to ensure that their entire value chain meets standards).

[102] *International Businesses To Produce a Global Privacy Code*, PRIVACY L. & BUS. INT'L NEWSL., http://worldlii.org/int/journals/PLBIN/2000/3.html (last visited Oct. 5, 2013).

[103] NICK MANSFIELD, INT'L COMMERCE EXCH., ICX PRIVACY AND DATA PROTECTION CODE OF CONDUCT (2000) (copy on file with author).

[104] *Id.*

[105] *Id.*

[106] *See The ICX Privacy Code of Conduct*, ICX, http://www.icx.org.uk/resources/res_0452.htm (last visited June 14, 2013).

It is harder to know how much weight to give to the theorists' concerns that self-regulation will result in lenient standards, insufficient monitoring, and lax enforcement.[107] In the absence of a comprehensive analysis of international privacy self-regulation one can only look by analogy to domestic examples. This record is not encouraging. In the United States, consumers find it difficult to understand and compare company privacy policies and find it impossible to negotiate the terms of these policies with the companies that post them.[108] Sectoral privacy standards have also been less than successful. A study of a leading self-regulatory program for the behavioral advertising sector found serious deficiencies in monitoring and enforcement.[109] An industry group is currently seeking to improve on this effort[110] and the jury is still out on whether it will succeed.[111] But the experience thus far does not instill confidence that self-regulation, much less *international* self-regulation, will deliver protective standards and high compliance. As two leading commentators have observed, "the incentive to breach privacy rules and, in particular, to collect, process, and disclose personal information without consent will tend to overwhelm the desire to be privacy-friendly."[112]

---

[107] *See infra* notes 109–112 and accompanying text.

[108] Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now Is the Time*, 1 CASE W. RES. J.L. TECH. & INTERNET 1, 26–27 (2009). *See* Tal Z. Zarsky & Norberto Nuno Gomes de Andrade, *Regulating Identity Intermediaries: The "Soft eID" Conundrum*, 74 OHIO ST. L.J. 1335, 1392–93 (2013).

[109] *See* Hirsch, *Online Privacy*, *supra* note 76, at 459–64 (discussing this research); *see also* BENNETT & RAAB, *supra* note 80, at 171 ("[C]ritics remain skeptical that . . . self-regulatory rules will be applied forcefully."); Pam Dixon, World Privacy Forum, The Network Advertising Initiative: Failing at Consumer Protection and at Self-regulation 2 (presented at the FTC Workshop, Nov. 1–2, 2007), *available at* http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf (analysis of Network Advertising Initiative self-regulatory program).

[110] This is the Digital Advertising Alliance's Self-regulatory Program for Online Advertising. *See The Self-regulatory Program for Online Behavioral Advertising*, DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info/ (last visited Sept. 16, 2013); *see also* Katy Bachman, *New Study Says DAA's Privacy Program Falls Short*, ADWEEK (Apr. 4, 2012), http://www.adweek.com/news/technology/new-study-says-daas-privacy-program-falls-short-139400.

[111] Initial studies have found a "significant gap in compliance" with important aspects of the standard. *See* SARANGA KOMANDURI, RICHARD SHAY, GREG NORCIE, BLASE UR & LORRIE FAITH CRANOR, CARNEGIE MELLON UNIV. CYLAB, ADCHOICES? COMPLIANCE WITH ONLINE BEHAVIORAL ADVERTISING NOTICE AND CHOICE REQUIREMENTS § 5.1 (2011), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11005.pdf (study of compliance with DAA AdChoices program). Initial studies have also found that a significant percentage of consumers do not understand the notice and choice messages provided to them. *See* PEDRO GIOVANNI LEON, JUSTIN CRANSHAW, LORRIE FAITH CRANOR, JIM GRAVES, MANOJ HASTAK, BLASE UR & GUZI XU, CARNEGIE MELLON UNIV. CYLAB, WHAT DO ONLINE BEHAVIORAL ADVERTISING DISCLOSURES COMMUNICATE TO USERS? 1, 2 (2012), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf (study of consumer understanding of DAA AdChoices icon).

[112] BENNETT & RAAB, *supra* note 80, at 171.

Self-regulation, like direct government regulation, may not be the best vehicle for establishing cross-border privacy rules.

C. *Co-regulation*

That may explain why policymakers are focusing so heavily on "co-regulatory" initiatives in which government and industry expressly and intentionally share responsibility for drafting, monitoring, and enforcing privacy standards.[113] Proponents of co-regulation argue that it combines the advantages of self-regulation with those of direct regulation. Like self-regulation, co-regulatory methods such as enforceable codes of conduct allow industry to draft the specific privacy rules.[114] They therefore draw on industry knowledge and expertise in much the same way that self-regulation does.[115] They are also more likely to get industry to accept and buy in to rules that they or their peers have drafted.[116] Like direct regulation, co-regulatory strategies generally call on government to establish the privacy framework to which all industry-drafted rules must conform.[117] They also get regulators involved in assessing, monitoring compliance with, and enforcing these rules.[118] This government involvement increases the chances that the rules will truly protect the public

---

[113] MARSDEN, *supra* note 76, at 46; Gunningham & Rees, *supra* note 76, at 366; Rubinstein, *supra* note 76, at 357.

[114] Stewart, *supra* note 91, at 82.

[115] NEIL GUNNINGHAM & DARREN SINCLAIR, LEADERS AND LAGGARDS: NEXT-GENERATION ENVIRONMENTAL REGULATION 104 (2002); Daniel J. Fiorino, *Toward a New System of Environmental Regulation: The Case for an Industry Sector Approach*, 26 ENVTL. L. 457, 483, 485 (1996) (stating that a negotiated, sector-based approach can allow "companies to tailor rules to their own circumstances"); Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 22, 27 (1997) (discussing "collaborative governance" as a form of co-regulation); Philip J. Harter, *Collaboration: The Future of Governance*, 2009 J. DISP. RESOL. 411, 418–20.

[116] GUNNINGHAM & SINCLAIR, *supra* note 115, at 108–09; Freeman, *supra* note 115, at 12, 23–24. A study of Dutch data protection codes of conduct has shown that some co-regulatory mechanisms may not be as flexible and adaptable as industry self-regulation. In the Netherlands, industry sectors draft a code of conduct and submit it to the regulator, which must approve it. *See* Dennis D. Hirsch, *Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law*, 2013 MICH. ST. L. REV. 83, 116 [hereinafter Hirsch, *Going Dutch*]. This generally requires each of the parties to make a substantial investment in an in-depth negotiation before they can reach agreement on the terms of the code. *See id.* at 133–34 & n.339–42. This makes them reluctant to re-open the terms of the agreement and so leads to static codes of conduct that generally do not change during their five-year term. *See id.* at 134–35, 156. In self-regulation, industry sets its own rules and does not have to obtain government approval of them. *Id.* at 99 n.97. This makes it easier for industry to re-open and revise these rules in order to account for changing technological or business realities.

[117] Rubinstein, *supra* note 76, at 357.

[118] GUNNINGHAM & SINCLAIR, *supra* note 115, at 108–09.

interest, and that companies will comply with them.[119] In sum, co-regulation promises rules that are stringent, intelligent, and up-to-date, that government enforces and industry accepts. This is an attractive picture for an area like privacy law where technologies and business models change too quickly for direct regulation, but where the stakes are too high to rely solely on industry self-regulation.

Co-regulation also has weaknesses. It envisions a government–industry negotiation over rules. Such regulation through "deal-making" can lead to sweetheart deals that favor industry interests over those of the public.[120] Much depends on how well the government regulators are able to exercise their authority (the company needs their approval, after all) and push back against company desires for less rigorous rules. Public interest stakeholders can counter industry influence. Including them in the discussion can increase the chances of a well-balanced set of rules.[121] Another weakness is that co-regulation can sometimes provide certain companies with an advantage over others. Insofar as the approach allows individual companies to draft their own codes of conduct and negotiate them with the regulators, this could lead to some companies having more advantageous arrangements and some less.

Finally, co-regulation may be less nimble and adaptive than self-regulation. In self-regulation, industry can develop, update, and change its rules all on its own. It does not need government approval to do so. In co-regulation, industry and government generally invest significant time and resources to reach agreement on a set of rules. This often makes them hesitant to reopen negotiations in order to update the rules. In at least one important example of privacy co-regulation, the negotiated industry codes of conduct largely remained unchanged over their five-year initial term.[122] Government and industry negotiators reconvened to update the code only when the expiration of the code required them to do so.[123]

IV. CURRENT INITIATIVES

Policymakers appear to believe that co-regulation's strengths outweigh its weaknesses. The three leading cross-border privacy rule initiatives all employ co-regulatory enforceable codes of conduct. These are: Binding Corporate Rules (BCRs), APEC Cross-border Privacy Rules (CBPRs), and the U.S.–E.U. Safe Harbor Agreement.

---

[119] *Id.*

[120] *Id.* at 105 ("[Collaborative negotiations] generate risks of a phenomenon tantamount to regulatory capture . . . .").

[121] *See infra* notes 192, 194–195 and accompanying text (discussing how best to integrate stakeholders into the negotiation process).

[122] Hirsch, *Going Dutch*, *supra* note 116, at 134.

[123] *Id.* at 134–35.

A. *Binding Corporate Rules*

Article 25 of the 1995 Data Protection Directive allows companies to transfer personal data from an E.U. member state to a non-E.U. nation only where the laws of the non-E.U. nation "ensure[] an adequate level of protection."[124] This requirement can pose a significant obstacle for multinational companies that wish to transfer personal data between operations in the E.U. and those in countries that have not yet passed laws establishing "adequate" privacy protections.

BCRs provide a way to accomplish such transfers without violating the Directive.[125] The multinational company creates a legally-binding set of rules[126] (which can take the form of a code of conduct) that, if followed, provides "adequate" protections for personal information. It commits that its entire corporate group—including its operations in non-E.U. nations—will be bound by and will follow these rules. It then submits these BCRs to a "lead DPA [data protection authority]" which evaluates whether, in fact, the rules provide "adequate" protection.[127] In making this assessment, the lead DPA consults with, and receives comments from, the DPAs of other member states in which the company operates.[128] If, after receiving these comments, the lead DPA determines that the corporate rules do, in fact, provide an "adequate" level of protection, it approves them.[129] The company can then transfer personal data among its various E.U. and non-E.U. operations without violating the Article 25 adequacy requirement so long as it does so in compliance with the approved rules. This is co-regulation in the sense that the company and the relevant DPAs work together to negotiate and craft the rules.

BCRs create a legal safe harbor with respect to the Article 25 adequacy requirement. That is their key function. However, they do not necessarily create a safe harbor with respect to the data protection laws of specific E.U. member states, nor do they necessarily do so with respect to the laws of the non-E.U. nations to which the company transfers the data.[130] This limits BCRs' ability to create global privacy rules. Compliance with a set of approved BCRs ensures only that the company complies with the Article 25 adequacy requirement when it transfers personal information outside of the E.U. It does not guarantee that the corporation is in compliance with the relevant national data protection laws.[131] Thus, a company with an approved BCR must still undertake the costly

---

[124] 1995 Directive, *supra* note 47, art. 25.

[125] CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 219 (2007).

[126] *Id.* at 219, 225.

[127] *Id.* at 223.

[128] *Id.* at 223–24.

[129] *Id.* at 227.

[130] *Id.* at 220.

[131] European Comm'n, Article 29 Data Prot. Working Party, *Working Document on Frequently Asked Questions (FAQs) Related to Binding Corporate Rules*, at 6, 1271-04-

task of studying and complying with a variety of different data protection laws; and regulators, individuals, and others seeking to evaluate that company's compliance still face the uphill battle of determining which jurisdiction applies and whether the firm is in compliance with that particular set of laws. BCRs are further limited in that they are valid only within the corporate group for which the DPAs have approved them.[132] They do not cover transfers from members of that group to other entities outside the group.[133]

B. *APEC Cross-border Privacy Rules*

Companies in the Asia-Pacific region also seek to transfer data across national borders. Asia-Pacific Economic Cooperation forum (APEC), an organization of twenty-one Asian and Pacific Rim countries including the United States, Canada, Japan, China, Russia, Mexico, and Chile, among others,[134] has developed a regulatory initiative to facilitate these transfers. Like the BCR program, the APEC Cross-border Privacy Rules (CBPR) initiative relies heavily on co-regulatory codes of conduct.[135]

The APEC approach is rooted in a set of Privacy Principles that all APEC member states have endorsed.[136] A participating company prepares a code of conduct or other set of "cross-border privacy rules" that explains how the APEC Privacy Principles apply to its specific operations.[137] It then submits this code to an APEC-approved Accountability Agent.[138] The Accountability Agent, which may be a government body or an independent third party, reviews the code to ensure that it properly fulfills the APEC Privacy Principles. If the Agent finds the code to be satisfactory, it approves it.[139]

02/08/EN, WP 155 rev.04 (Apr. 8, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf; KUNER, *supra* note 125, at 220.

[132] KUNER, *supra* note 125, at 227.

[133] *Id.*

[134] *See History*, APEC, http://www.apec.org/About-Us/About-APEC/History.aspx (last visited July 15, 2013); *Member Economies*, APEC, http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (last visited July 15, 2013) (listing the current member countries).

[135] *See* Asia-Pac. Econ. Cooperation, *APEC Data Privacy Pathfinder Projects Implementation Work Plan—Revised*, 2009/SOM1/ECSG/SEM/027 (2009), *available at* http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx.

[136] *See generally* APEC, *APEC Privacy Framework*, at 3, APEC#205-SO-01.2 (2005) [hereinafter *APEC Framework*], *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.aspx (listing the APEC Privacy Principles); see also Table 3, *infra* Part V.B.2, for an overview of these Principles.

[137] Paula J. Bruening, *APEC Roundup: Update on Accountability Agents in Implementation of the APEC Framework, Development of Pathfinder Projects, More*, 9 PRIVACY & SECURITY L. REP. (BNA) 1444 (Oct. 18, 2010).

[138] *Id.*

[139] *Id.*

This approval has an ambiguous legal meaning. It does not provide the company with a safe harbor with respect to national laws. Even those companies with approved codes are still subject to the privacy laws of the individual APEC nations.[140] That said, companies that follow an APEC-approved code of conduct can feel more comfortable than they otherwise would that their behavior complies with the laws of APEC member states or that, even if it turns out that they do not, these countries will not enforce their laws as harshly as they otherwise would. Thus, APEC privacy codes provide some comfort to firms that engage in cross-border transfers among APEC states. It remains to be seen whether this is sufficient incentive to encourage companies to develop an APEC privacy code and whether such a system truly will facilitate cross-border data transfers.

C. *The U.S.–E.U. Safe Harbor Agreement*

The U.S.–E.U. Safe Harbor Agreement, too, uses company codes of conduct to address a cross-border data transfer issue. The U.S. Department of Commerce and the European Commission developed the Safe Harbor Agreement to respond to the 1995 Directive's "adequacy" requirement which, once U.S. laws were deemed to be "inadequate," promised to disrupt vital data transfers between the two trading partners.[141] The Safe Harbor Agreement seeks to address this problem and facilitate cross-border data flows between the E.U. and the United States.[142]

The Agreement defines a set of principles—the Safe Harbor Privacy Principles—that both E.U. and U.S. officials agree approximate the requirements of E.U. data protection law.[143] Under the Agreement, a company can develop its own set of privacy and data governance practices—essentially, a code of conduct—that translates the Safe Harbor Principles and explains how the company will comply with them. Alternatively, it can join a safe harbor

---

[140] *APEC Cross-border Privacy Rules System: Policies, Rules and Guidelines*, APEC, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx (last visited Sept. 16, 2013) ("The CBPR System does not displace or change an Economy's domestic laws and regulations. . . . Participation in the CBPR System does not replace a participating organization's domestic legal obligations. . . . Where domestic legal requirements exceed what is expected in the CBPR System, the full extent of such domestic law and regulation will continue to apply."); *accord* Justin Brookman, *Can "Cross-border Privacy Rules" Trump Divergent Data Protection Laws?*, CENTER FOR DEMOCRACY & TECH. (Oct. 4, 2011), https://www.cdt.org/blogs/justin-brookman/410can-"cross-border-privacy-rules"-trump-divergent-data-protection-laws (explaining the APEC framework explicitly requires compliance with various national data protection laws).

[141] Rubinstein, *supra* note 76, at 390–91.

[142] *See U.S.–EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated July 1, 2013, 8:51 AM).

[143] *See* Dep't of Commerce, *Safe Harbor Privacy Principles*, EXPORT.GOV (July 21, 2000), http://export.gov/safeharbor/eu/eg_main_018475.asp.

"self-regulatory privacy program," such as TRUSTe's E.U. Safe Harbor Seal Program, that guides companies on how to comply with the Safe Harbor Principles.[144] Individual companies self-certify to the Department of Commerce and in their own posted privacy policy that they are in compliance with the Safe Harbor Principles.[145] So long as they meet this commitment, companies are deemed to provide "adequate" protection for the purposes of the 1995 Directive and can transfer personal data to and from the E.U. Firms that fail to follow through are subject to FTC enforcement under Section 5 of the FTC Act for engaging in a "deceptive" business practice.[146] Companies that fail to sign up for the Safe Harbor program altogether are deemed not to provide "adequate" protection and are, in theory, prohibited from processing the personal data of E.U. citizens.

The U.S.–E.U. Safe Harbor Agreement is similar in many ways to BCRs and APEC CBPRs. Each requires a government official or representative to approve an industry-drafted code of privacy practices. Each provides some degree of legal protection to firms that comply with such a code. One salient difference is that, while the BCR and APEC CBPR initiatives currently work only at the level of the individual company, the Safe Harbor program also recognizes self-regulatory privacy programs (e.g. TRUSTe) that operate at the economy-wide level. Many different companies, from a variety of economic sectors, may "join" such an organization and follow its guidelines on compliance with the Safe Harbor Principles. Thus, while the BCR and CBPR initiatives constitute co-regulation at the company level, the U.S.–E.U. Safe Harbor Agreement includes both company level and economy-wide co-regulation.

D. *The Current Initiatives Share a Common Weakness*

The current initiatives—BCRs, CBPRs, and the U.S.–E.U. Safe Harbor Agreement—share some common virtues. They provide companies (and, in the case of the Safe Harbor Agreement, self-regulatory privacy programs such as TRUSTe) with a means to create an approved, cross-border set of privacy rules. And they do this through a co-regulatory mechanism that utilizes industry knowledge to produce intelligent rules. Each works only with respect to certain borders (for BCRs, the borders of the E.U.; for CBPRs, those of APEC member nations; and for the Safe Harbor Agreement, those between the E.U. and the United States), and so none provides a truly global solution. Still, each takes an important step toward the goal of broadly applicable, cross-border privacy rules.

The three initiatives also suffer from the same fundamental weakness: *They rely on individual companies, rather than industry sectors, to draft the cross-*

---

[144] *Id.*; *see also Datasheets*, TRUSTE, http://www.truste.com/resources/#/Datasheets (last visited Oct. 5, 2013) (describing TRUSTe's role).

[145] Rubinstein, *supra* note 76, at 391.

[146] *Id.*; Dep't of Commerce, *supra* note 143.

border privacy rules.[147] That is, they are company-based codes rather than sector-based ones. This has a number of important drawbacks that those who promote and write about cross-border privacy rules do not as yet appear to have grappled with.

To begin with, it is expensive to write a comprehensive privacy code and negotiate it with the relevant authority. Only the largest and most sophisticated companies have the resources and expertise to do this.[148] Small- and medium-sized businesses, and even some large companies, will not be able to develop their own company-specific code of conduct that meets the requirements of the 1995 Data Protection Directive, APEC Privacy Principles, or U.S.–E.U. Safe Harbor Agreement.[149] As a consequence, only the largest and most knowledgeable companies will be able to take advantage of BCRs, CBPRs, and the Safe Harbor Program (unless they participate in a Safe Harbor self-regulatory privacy program, the drawbacks of which are detailed below).[150] The roster of companies that have successfully negotiated the BCR process bears this out. The list of forty-six companies includes such firms as Accenture, American Express, British Petroleum, Citigroup, eBay, General Electric, ING Bank, and Shell International.[151] What about all the other, smaller companies that transfer personal data between and among E.U. member states but cannot afford to draft and negotiate a BCR? They are left without a streamlined mechanism for compliance with E.U. "adequacy" requirements. The same can be said for the APEC CBPRs and for the U.S.–E.U. Safe Harbor Agreement insofar as it uses company codes of conduct.[152]

Were more firms to become able to take advantage of "company-based" codes (so named because they are drafted and negotiated at the level of the individual company or firm), this would create another large problem—high administrative costs for regulators.[153] DPAs (in the case of BCRs) and government agencies serving as APEC Accountability Agents would have to

---

[147] The Safe Harbor Agreement also employs economy-wide sets of privacy rules, i.e., those developed by safe harbor organizations and open to companies from any economic sector. These are also flawed, as explained *infra*.

[148] KUNER, *supra* note 125, at 220 ("[T]he [BCR] approval process can be lengthy, and implementation can be expensive and difficult for all but large multinationals.").

[149] *Cf.* Priest, *supra* note 77, at 258 (asserting small companies find it burdensome to engage in self-regulation).

[150] *See infra*.

[151] See the listing of those companies that have completed the BCR process that is available at *List of Companies for Which the EU BCR Cooperation Procedure Is Closed*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last updated Aug. 26, 2013).

[152] *Cf.* Priest, *supra* note 77, at 281 (concluding company-based approaches to self-regulation lead to disparate obligations for different firms).

[153] *Id.* at 258 (stating firm-based self-regulation makes it "more costly" for government regulators); *id.* at 278 (explaining individuated, company-based self-regulatory regime compromises efficiency).

review, negotiate, and approve an individual code for every company that wanted to engage in an international data transfer. This would present a significant, possibly insurmountable, burden for these resource-strapped public bodies. The APEC CBPR program seeks to minimize this by anointing independent "Accountability Agents" to review and approve the codes. But this has a downside of its own in that, insofar as Accountability Agents are private rather than public entities, they may not sufficiently protect the public interest.

Company-based codes also suffer from another problem: they frustrate public participation and so reduce accountability. Privacy NGOs have even fewer resources than regulatory agencies. If a significant number of companies were to submit codes for the BCR or CBPR programs or self-certify compliance with a code under the Safe Harbor program, stakeholders would lack the resources to keep track of, much less participate in, the many submissions, negotiations, and approvals.[154] Company-specific codes will escape public scrutiny by overwhelming it with sheer numbers.

Of course, it may turn out that only a small number of companies have the resources and sophistication to establish firm-based, cross-border rules. If so, then regulators and stakeholders may be able to manage supervision of these codes. But the small number of participating companies will exacerbate the first problem identified—the uneven playing field between those large companies that are able to draft and negotiate their own set of cross-border privacy rules, and the small- and medium-sized enterprises that lack the resources and expertise to do so. This will hurt the very start-up and emerging companies on which the information economy depends for innovation.

Before leaving this topic, it is important to note that while companies can develop their own code that meets the Safe Harbor Principles, self-regulatory privacy programs also exist to educate such companies on the Principles and guide them through the self-certification process.[155] This could allow many companies to come together under the banner of a single safe harbor organization, such as TRUSTe, and so reduce the resource and administrative burdens associated with code drafting and approval. This "economy-wide" approach to cross-border codes (so named because safe harbor organizations, eager for members, are generally open to companies from any sector of the economy) mitigates one set of problems but replaces it with another. As regulatory theorists have explained, the principal virtue of industry-drafted codes of conduct is that they are able to tap into private sector knowledge and produce rules that are tailored to the realities of the business world.[156] When a company or trade association that represents a particular sector drafts a code, it generally achieves this benefit. Companies and sectors have particular realities that characterize them, and the drafters can tailor a code to address them. By

---

[154] Stakeholders typically have even fewer resources to devote to this task than government agencies do.

[155] *See supra* note 144 and accompanying text.

[156] *See supra* note 115 and accompanying text.

contrast, when a safe harbor organization or other such entity offers an *economy-wide* approach open to companies from many different sectors, it is not able to tailor it to particular realities. Such interpretations of the Safe Harbor Principles must, necessarily, remain broad enough to encompass firms from many different lines of business that have divergent characteristics. They will therefore fail to take advantage of the principal attribute of codes of conduct and the main reason why policymakers look to them—the ability to draw on firms' knowledge of their own particular realities and tailor the rules to account for them.

V. SECTOR-BASED PRIVACY CODES: A BETTER SOLUTION

There is another way to structure cross-border, co-regulatory codes of conduct. Industry sectors could draft them. They could then submit these sectoral codes to the relevant national and regional governments for approval. Once these governments approved the code, individual firms that complied with it would be in compliance with the laws of each of the approving jurisdictions. The sectoral code would serve as an international set of privacy rules for companies within its sector.

Employing sector-based—as opposed to company-based or economy-wide—codes of conduct would ameliorate many of the problems that the other two approaches produce. Sector-based codes would be accessible, not only to the largest and most sophisticated firms, but to small- and medium-sized ones as well. Such smaller companies could organize themselves—either through a trade association or otherwise—and pool their resources to support the drafting and negotiation of a code of conduct for their sector. This would make participation in a sector-based code system feasible for such companies in a way that developing a company-based code would not be. More companies would accordingly have access to sector-based codes than to company-based ones.

A sector-based system would also reduce regulators' administrative costs. There are fewer sectors than there are companies. Concentrating the code negotiation process at the level of the sector would therefore reduce the resources needed to supervise and engage in this process. Sector-based codes should also be more amenable to public participation than their company-based counterparts. Stakeholder organizations will have a smaller number of codes to review and monitor. These groups should find this to be a much more manageable task. For all of the above reasons, sector-based codes would likely function better than the company-based codes on which the current initiatives rely so heavily.

They also stack up well against the economy-wide approach that the Safe Harbor program utilizes. Economy-wide interpretations of the Safe Harbor Principles must speak in broad terms so that many different types of companies

can utilize them.[157] They cannot tailor themselves to the specific realities of a company or sector. Sector-based codes, on the other hand, can do this. The drafters of a sector-based code—for example, a trade association that represents that sector—can draw on the experience and knowledge of companies in that branch of industry. They can build this into the code and so produce a document that intelligently accounts for the specific technological and business realities of that particular sector.[158] Sector-based codes will possess the most important advantages of company-based and economy-wide codes while avoiding their most significant weaknesses. Initiatives seeking to establish cross-border privacy rules should employ sector-based codes in place of, or in addition to, these other two types of codes. The following table depicts the current initiatives and where the recommended sector-based approach would fit among them.

Table 2: *Cross-border Privacy Rules*

	Direct Regulation	*Self-regulation*	*Co-regulation*
Company-Based	International treaty implemented through national law	Corporate privacy policies	BCRs CBPRs Safe Harbor
Sector-Based	International treaty	(Network Advertising Initiative)[159]	**Proposed approach**
Economy as a Whole	International treaty	ICX Code	Safe Harbor

A. *Achieving International Privacy Rules Through Sector-Based Codes: An Implementation Strategy*

There is precedent for using sector-based codes of conduct in privacy law. Dutch data protection regulation relies heavily on them. The Netherlands has a national privacy law, the Personal Data Protection Act.[160] However, the Dutch DPA does not promulgate regulations to implement the Act. Instead it invites

[157] *See supra* notes 155–156 and accompanying text.

[158] BENNETT & RAAB, *supra* note 80, at 156 ("Sectoral codes permit . . . a more refined set of rules tailored to the issues within each industry.").

[159] The Network Advertising Initiative is a group of more than ninety online advertising companies that has adopted a code of conduct for protecting consumer privacy in interest-based advertising. *See* NAI: NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/ (last visited Oct. 5, 2013) (describing the NAI and providing a link to the 2013 NAI code of conduct). The purpose of this sector-based self-regulatory organization is to encourage best practices among industry members and so, perhaps, to obviate the need for direct government regulation of behavioral advertisers. NAI thus has a domestic rather than an international focus. Still, it can serve as an example of a self-regulatory, sector-based code.

[160] Wet bescherming persoonsgegevens, Stb. 2000, p. 302, ch. 3, art. 25 (Neth.).

industry sectors, usually represented by a trade association, to draft codes of conduct that apply the Act to the realities of their specific sector.[161] Once the Dutch DPA approves a given code, any company in that sector that complies with it inhabits a legal safe harbor with respect to the statute.[162] The Dutch DPA has approved twenty sector-based codes of conduct including codes drafted by the pharmaceutical, banking, insurance, direct marketing, and credit rating industries.[163] These codes are tailored to the business realities of the specific sectors that they govern.[164]

The Dutch program can serve as a model for the establishment of cross-border, sectoral privacy rules. Such an international initiative would work as follows. First, an industry sector would draft a code of conduct that complies with the E.U.'s 1995 Data Protection Directive and with the APEC Privacy Principles, and that tailors these requirements to its particular realities. Next, the sector would submit the code to European authorities who would review it for compliance with the 1995 Directive. If these officials approved it, then individual companies that followed the terms of the code would be deemed to be in compliance with the data protection laws of all twenty-eight E.U. member states. The code would constitute a legal safe harbor with respect to all E.U. member states and would represent "adequate" protection for data transferred outside the E.U.

The sector would then take the same code and submit it to an APEC Accountability Agent who would review it for compliance with the APEC Privacy Principles. If the Agent approved the code, then it would constitute a legal safe harbor (or something close to it) with respect to the twenty-one APEC member economies, including the United States, China, Japan, and Russia. Once this happened, companies that followed the twice-approved code could transfer data across borders with confidence that they were complying with the laws of the most significant European and Asian-Pacific nations. The code would constitute a nearly global set of cross-border privacy rules.[165]

Is such an approach realistic? To assess this it is important, first, to examine the E.U. and APEC systems on the level of *process*. Does each system have procedures in place that would allow it to approve a sector-based code? If so, would this act truly create a legal safe harbor for companies that followed the

---

[161] *See* Hirsch, *Going Dutch*, *supra* note 116, at 116 (describing this feature of the Dutch data protection code of conduct program).

[162] *Id.* at 122 ("They (the Dutch) implement, and create a safe harbor with respect to, all statutory requirements.").

[163] *Id.* at 89 & n.27, 162–66 (providing Appendix that identifies all twenty approved Dutch codes).

[164] *Id.* at 103 n.121, 157–58 (providing examples of such tailoring).

[165] It would leave out parts of South America and Africa for which there is not yet a regional organization that could approve such a code. This is an important omission insofar as it could increase the costs of doing business in these areas as compared to those in which regional authorities had approved the code. One solution would be for South America and Africa to develop regional privacy organizations similar to APEC that could adopt privacy principles and approve codes consistent with these principles.

approved code? Next, it is important to examine the E.U. and APEC systems with respect to *substance*. Are these systems' privacy requirements sufficiently congruent that a single code could integrate them into a single set of rules? Or do they conflict with one another such that it is not possible to combine them in this way? The remainder of this section will analyze the proposed strategy on the levels of both process and substance.

B. *Global Codes: Process*

Do the E.U. and APEC systems have a process for approving sector-based codes of conduct?

1. *E.U. Approval*

In seeking to answer this question with respect to the E.U. system, it is important to look both at E.U. law as it exists today (i.e., the 1995 Data Protection Directive) and as it is likely to be in a few years' time (i.e., the proposed General Data Protection Regulation). Under either scenario, E.U. law should offer a clear mechanism for evaluating and approving sector-based codes that, if approved, will constitute a legal safe harbor with respect to all E.U. member nations.

a. *The 1995 Data Protection Directive*

Article 27 of the 1995 Directive expressly authorizes "trade associations" representing a branch of industry to draft a code of conduct and submit it to the Article 29 Working Party.[166] The Working Party "shall determine . . . whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive."[167] If they are, the Directive instructs the Working Party to "approve[]" the code and the European Commission to publicize this approval.[168] Such an approved, E.U.-wide code is known as a "Community Code."[169] A Community Code differs from a BCR in that it constitutes a legal safe harbor with respect to the laws of all twenty-eight E.U. member states, whereas BCRs ensure compliance only with the Article 25 "adequacy" requirement. It also differs in that a Community Code is proposed by and applicable to an industry *sector*, whereas a BCR is proposed by and applicable to an individual *company*. Given that a Community Code represents compliance with the data protection laws of all E.U. member states, a multinational company that followed a Community Code throughout its operations should

---

[166] 1995 Directive, *supra* note 47, art. 27(2)–(3).
[167] *Id.* art. 27(3).
[168] *Id.*
[169] *Id.*

also meet the Article 25 "adequacy" test. So long as all of its corporate groups complied with the Code, it should be able to freely transfer data outside the E.U.

The Federation of European Direct and Interactive Marketing's (FEDMA) Community Code provides an example of how this process would work. FEDMA drafted and proposed a Community Code.[170] In 2003, the Article 29 Working Group approved it.[171] The code incorporates the requirements of the 1995 Directive and tailors them to the particular realities of the direct marketing industry.[172] It provides a legal safe harbor, valid with respect to the data protection laws of all twenty-eight E.U. member states, for any European direct marketing firm that complies with it. In 2010, the Article 29 Working Party approved an "annex" to the FEDMA code that covers online marketing.[173]

It is worth noting that the direct marketing industry is the only sector that has successfully established a Community Code. This underutilization of the Article 27 Community Code process is likely a reflection of the significant costs involved in drafting and negotiating a code of this type. Still, the Article 27 process, as illustrated by the Article 29 Working Party's approval of the FEDMA code, appears to provide just the process needed to establish sector-based, international privacy rules that would function throughout the E.U. In theory, any sector could propose such a code to the Article 29 Working Party. If the Working Party approved it, the code would provide a legal safe harbor with respect to the data protection laws of all E.U. member states. Thus, at least with respect to the European Union, a clear process exists for implementing E.U.-wide, sector-based privacy codes.

b. *The Proposed General Data Protection Regulation*

European data protection law is in flux. On January 25, 2012, the European Commission proposed a new General Data Protection Regulation that, if adopted, would replace the 1995 Data Protection Directive.[174] The proposed General Regulation would be directly binding on regulated parties in the E.U. and so would harmonize data protection law throughout the European Union.

---

[170] *See* European Comm'n, Article 29 Data Protection Working Party, *Opinion 3/2003 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing*, at 3, 10066/03/EN final, WP 77 (June 13, 2003), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp77_en.pdf.

[171] *See id.*

[172] *See id.* at 3–4.

[173] *See* European Comm'n, Article 29 Data Protection Working Party, *Opinion 4/2010 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing*, at 2–3, 00065/2010/EN, WP 174 (July 13, 2010), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf.

[174] *See Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Proposed General Regulation*].

This new set of laws, or some version of it, is likely to replace the 1995 Directive within the next few years.

Like the 1995 Directive, the proposed General Regulation provides a means for developing E.U.-wide, sector-based codes of conduct. Article 38 of the proposed Regulation (January 25, 2012 draft) requires national supervisory authorities and the European Commission to "encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors."[175] Where the association proposing the code represents data controllers in a number of different member states (as would be the case in the strategy that this Article proposes), the proposed Regulation allows the organization to "submit draft codes of conduct . . . to the Commission."[176] It gives the Commission (i.e., the European Commission) the authority to "adopt implementing acts for deciding that the codes of conduct . . . submitted to it . . . have general validity within the Union."[177]

This proposed procedure appears in many respects similar to the one that Article 27 of the 1995 Directive currently makes available. It allows trade associations to submit sector-based codes of conduct to the Commission. It authorizes the Commission to approve such codes and so to give them "general validity" throughout the European Union. The only meaningful difference is that, under the 1995 Directive, the Article 29 Working Party reviews and approves the code whereas, under the proposed General Regulation, the Commission handles this task. But other than that, the proposed Regulation, in its current form at least, keeps in place the process now available under Article 27 of the 1995 Directive for the approval of Community Codes. In conclusion, both existing and proposed E.U. data protection laws appear to provide exactly the process needed to establish legally approved, E.U.-wide, sector-based codes of conduct.

2. *APEC Approval*

It is far less clear whether the APEC Privacy Framework, as currently constituted, would support the approval of sector-based codes. The APEC CBPR program allows individual *companies* to submit codes of conduct to an Accountability Agent and to seek the Agent's approval that the code complies with the APEC Privacy Principles. But nothing in APEC's published procedures suggests that an *industry sector* could submit such a code and obtain approval of it. If sectors are to be able to utilize the E.U. and APEC processes to establish international privacy rules, it will be important for APEC expressly to open its process to sector-based codes. Absent such a change, large, sophisticated

---

[175] *Id.* art. 38(1).
[176] *Id.* art. 38(3).
[177] *Id.* art. 38(4).

companies will be able to take advantage of the APEC cross-border rules process but many small- and medium-sized enterprises will not.

The APEC process also falls short in its creation of a legal safe harbor. As explained above, APEC guidance makes clear that an Accountability Agent's approval of a company code *does not* guarantee compliance with the data protection laws of APEC member nations and *does not* create a legal safe harbor with respect to them.[178] This means that firms operating in the APEC framework will still have to track and comply with the data protection laws of many different nations; and regulators, individuals, or other stakeholders trying to check on compliance will find it hard to know which jurisdiction's rules apply at any given moment in personal data's cross-border journey. Thus, the APEC CBPR system will not fully address the problems that cross-border data transfers create for business, data subjects, or other stakeholders. This contrasts with the Article 29 Working Party's approval of a Community Code (or the Commission's approval of a sector-based code under the proposed Regulation), which clearly *does* create a legal safe harbor—and so a single set of rules—with respect to the entire E.U.

The APEC system needs to change in two ways in order to allow for the implementation of sector-based, cross-border codes. It needs to open up its code approval process to industry sectors. And it needs to increase the legal significance of Accountability Agent approval so that it more closely approximates a legal safe harbor. This will facilitate cross-border data transfers among the APEC nations. It will also enable the APEC and E.U. code approval systems to operate in concert with one another and so to produce cross-border privacy rules that encompass the E.U., the United States, and much of Asia.

C. *Global Codes: Substance*

This raises the second major question: can these two systems work in harmony? Is there sufficient substantive overlap? This is a tricky question because the law in this area is a moving target. The APEC Privacy Principles appear to be stable for now. But European data protection law is not. As was mentioned above, the European Commission has proposed a General Data Protection Regulation that would replace the 1995 Data Protection Directive.[179] The proposed Regulation would directly bind regulated parties in the E.U. and would not require member states to implement legislation. In this way, it would further harmonize E.U. data protection law. The General Data Protection Regulation will likely replace the 1995 Directive within the next few years.

U.S. privacy law is also in flux. To date, U.S. privacy law has consisted of targeted statutes that regulate specific sectors (e.g., health care, financial institutions). In recent years, members of the House and the Senate have proposed comprehensive commercial privacy legislation that would expand

---

[178] *See supra* note 140 and accompanying text.

[179] *See supra* note 174 and accompanying text.

U.S. privacy to all other economic sectors.[180] The Commercial Privacy Bill of Rights Act of 2011, a bipartisan bill introduced by Senator John McCain (R-Ariz.) and then-Senator John Kerry (D-Mass.), is the most developed of these legislative proposals and illustrates this legislative direction.[181] The Bill would establish a broad set of privacy requirements—the commercial privacy "Bill of Rights."[182] It would then allow sector-based trade associations (as well as other private entities) to develop a code that fleshes out the statute and applies it to their sector.[183] If the FTC were to agree that the code properly interprets the statute, and approve it, then the Bill would grant those firms that comply with the code a legal safe harbor analogous to the one that the E.U. provides for companies that follow an approved Community Code.[184] This is a far stronger safe harbor than the one that would otherwise be available to U.S. companies under the APEC CBPR system. While Congress is unlikely to pass comprehensive privacy legislation in the near future, another major controversy regarding commercial holdings of personal data, coming on top of the recent scandal involving National Security Agency access to private-sector phone and Internet records, could cause it to act.

This evolving picture complicates the analysis of whether comprehensive E.U., APEC, and (potentially) U.S. privacy laws overlap sufficiently for a cross-border code to incorporate the requirements of each. It requires that the analysis consider four bodies of privacy law: the 1995 Directive, the proposed General Data Protection Regulation, the APEC Privacy Principles, and the Commercial Privacy Bill of Rights Act (the congressional bill that has received the most attention and that best represents how U.S. privacy law may evolve in the future).

Table 3 depicts the substantive contours of the four existing and proposed sets of comprehensive privacy rules. The first column identifies the main types of privacy-protective requirements that such systems might include. Each of the subsequent columns is devoted to one set of privacy rules (the 1995 Directive, the proposed General Data Protection Regulation, the APEC Privacy Principles, or the Commercial Privacy Bill of Rights Act) and indicates whether that set of rules contains the listed privacy requirements. This allows one to see the extent to which these systems overlap with one another. Table 3 is reproduced in the Appendix with supporting citations, but for purposes of clarity it appears immediately below without footnotes.

---

[180] *See* Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. § 9 (2011); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); BEST PRACTICES Act of 2011, H.R. 611, 112th Cong. (2011).

[181] *See* S. 799.

[182] *See id.* §§ 101–303.

[183] *See id.* § 501.

[184] *See id.* §§ 501–02.

Table 3: *Substantive Overlap*[185]

Requirements	E.C. 1995 Directive	E.U. General Regulation	APEC Privacy Principles	U.S. Commercial Privacy Bill of Rights Act
Transparency of Data Practices	✓	✓	✓	✓
Choice/Consent	✓	✓	✓	✓
Legitimate Bases (Other than Consent)	✓	✓	✓	✓
Security Safeguards	✓	✓	✓	✓
Accuracy	✓	✓	✓	✓
Access	✓	✓	✓	✓
Correction	✓	✓	✓	✓
Purpose Limit on Use	✓	✓	✓	✓
Sensitive Data	✓	✓	(✓)	✓
Accountability		✓	✓	✓
Purpose Limit on Collection	✓	✓	✓	✓
Data Minimization	✓	✓		✓
Fair and Lawful	✓	✓	✓	
Retention and Disposal	✓	✓		✓
Privacy by Design		✓		✓
Prior Check	✓	✓		
Right To Object	✓	✓		
Automated Decisions	✓	✓		
Notification to Data Subject	✓	✓		
Children's Data Requires Parent's Consent		✓		(✓)
Data Protection by Default		✓		
Privacy Impact Assessment		✓		
Notification to Data Protection Authority	✓			
Documentation of Processing		✓		
Right To Be Forgotten and to Erasure		✓		
Data Portability		✓		
Preventing Harm			✓	✓
Data Protection Officer		✓		
Supervisory Authority	✓	✓		
"Adequacy" Limit for International Transfer	✓	✓		

[185] Table 3 is reproduced with supporting citations in the Appendix.

Table 3 shows that the four comprehensive systems of privacy rules do overlap in many of the most important areas.[186] Each system provides for (1) transparency with respect to data practices, (2) choice/consent, (3) legitimate bases for processing other than consent, (4) reasonable security safeguards, (5) accuracy, (6) access, (7) correction, (8) purpose limitations with respect to the use of personal data, (9) purpose limits with respect to the collection of personal data, and (10) special protections for sensitive data. In addition, three out of the four systems provide for (11) accountability, (12) data minimization, (13) fair and lawful processing, and (14) limits on retention and disposal of personal data. While Table 3 also shows that these systems differ in a number of ways, fourteen significant areas of overlap is a lot of common ground. Potentially, a sector could develop a code that addressed each of these requirements in a way acceptable to each of the relevant systems. Firms that complied with such a code would know that they met the most significant privacy requirements of each system.

In order to build in *all* the requirements of each system, such a code would need to go beyond the areas of overlap and include elements (e.g., data portability or the prevention of harm) that are currently present in only one or two of the systems. To be truly universal, such a comprehensive code would have to incorporate the most stringent requirements from each set of privacy rules. This would lead to a "ratcheting up" of requirements for companies that otherwise would only be subject to one such system or another. The increased efficiency to be gained from a single, nearly global set of privacy rules, as well as any enhanced consumer trust that their commitment to follow a stringent code may bring them, could provide firms with sufficient incentive to take such a step. The production and implementation of (nearly) global privacy codes could accordingly lead to an increase in privacy protections.

It is also important to qualify any conclusions drawn from Table 3 and to recognize what it cannot tell us. Table 3 lists only broad privacy requirements. It says nothing about how each system defines and interprets these requirements. For example, two systems may each require "consent" to the processing of personal data, thereby making it appear that they are similar. But further examination may show that one system allows opt-out consent across the board, while the other requires opt-in consent in certain situations.[187] A drafter seeking to put together a cross-border code would, accordingly, have to examine in detail the definitions, explanatory statements, and regulatory and applicable judicial interpretations in order to compose a requirement that would

---

[186] This should not be surprising given that these sets of laws share a common root: the eight basic principles of privacy protection as set forth in the Fair Information Privacy Practices that the U.S. Department of Health, Education and Welfare (HEW), and later the OECD, articulated. *See* Gerber, *supra* note 41 (setting forth the eight basic privacy principles as collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability).

[187] *Cf.* Reidenberg, *supra* note 2, at 1332–35 (describing instances in which jurisdictions subscribe to the same privacy principles but interpret them quite differently).

truly satisfy each of the relevant systems. While such an analysis is clearly needed in order to determine whether the various privacy rule systems can actually be combined into a single code, it is beyond the scope of this Article and will require additional research. Table 3 seeks only to provide a "first cut" at the analysis by determining whether the broad frameworks match up. It shows that, with respect to many important privacy requirements, they do. On the levels of both process and substance, the conditions are sufficiently favorable to warrant further exploration of this approach.

D. *Multi-stakeholder Codes of Conduct: The White House Approach*

In its 2012 report, *Consumer Data Privacy in a Networked World*, the White House expressed its enthusiasm for enforceable privacy codes of conduct.[188] It called for legislation that would establish a Consumer Privacy Bill of Rights,[189] allow private groups to implement them through a code of conduct,[190] and create a legal safe harbor where FTC approves such codes.[191] The White House expressed its intention to include "international stakeholders" in the discussions about particular codes of conduct so that the codes could come to reflect a "transatlantic consensus on important, emerging privacy issues."[192] It disclosed "plans to develop additional mechanisms—such as jointly developed codes of conduct—that support mutual recognition of legal regimes."[193]

On one level, these White House pronouncements parallel and reinforce some of this Article's key positions. The report envisions group-based codes—perhaps even sector-based codes—rather than individual company codes. It envisions using codes of conduct to "support mutual recognition of legal regimes." While this latter statement may be somewhat vague and undeveloped, it nonetheless shows an interest in using codes in this way. The White House report supports additional exploration of this approach to cross-border privacy rules.

The White House report also goes beyond this Article's analysis in ways that raise interesting questions about how best to implement the code negotiation process. The report calls for "multi-stakeholder" groups to develop the codes, and states that such groups will consist of "individual companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorney Generals, Federal civil and criminal law enforcement representatives, and other relevant groups."[194] These groups must

---

[188] THE WHITE HOUSE, *supra* note 63, at 23–29.
[189] *Id.* at i.
[190] *Id.* at 23.
[191] *Id.* at 37.
[192] *Id.* at 33.
[193] *Id.*
[194] THE WHITE HOUSE, *supra* note 63, at 23.

reach "consensus" on the code before companies can adopt it.[195] Clearly, stakeholders must be involved in the code negotiation process. But is such a large group workable? This is a far greater array of parties than negotiate the Dutch codes or the APEC Cross-border Privacy Rules.[196] The size and complexity of such groups raise questions about transaction costs and the ability to reach consensus on broad and meaningful requirements. Pursuant to the White House agenda, the National Telecommunications and Information Administration (NTIA) has for the past year been facilitating a multi-stakeholder process of this type to develop a code of conduct on Mobile App Transparency.[197] The process, which began with over 200 representatives present at the initial negotiation, has made important progress. However, it remains to be seen whether it can produce a meaningful code with a substantial number of adoptees.

Another difference is the White House's intention to proceed with multi-stakeholder codes of conduct *even in the absence* of comprehensive privacy legislation.[198] Under such a scenario, neither the FTC nor any other agency will independently assess and approve the code. Instead, the report envisions that the government's role be limited to "help[ing] the parties reach clarity," and that it not get involved in "substituting its own judgment" for that of the multi-stakeholder group.[199] This precludes the use of mutually *approved* codes of conduct that could create a cross-border legal safe harbor for firms that followed a code. It also means that the codes will not create a legal safe harbor—one of the key attractions for industry. Will such a code be able to attract a sufficient number of industry participants? Again, the NTIA's current experiment with the multi-stakeholder negotiation over Mobile App Transparency appears to be a valuable one that could provide important lessons about this regulatory approach.

VI. RECOMMENDATIONS

Part II of this Article showed that a world of increasingly global data flows needs cross-border privacy rules to foster the Internet economy and protect individual privacy. Part III began by posing two questions about how to design such a system: (1) who should regulate? and (2) at what level should they regulate? It is now possible to answer these questions. Who should regulate? Government and industry should regulate together. Co-regulation is likely to be

---

[195] *Id.* at 27.

[196] For the APEC CBPRs, a single company negotiates the code with the Accountability Agent. *See supra* Part IV.B. The Dutch codes are negotiated by trade associations representing companies from the same sector. *See* Hirsch, *Going Dutch*, *supra* note 116, at 89.

[197] *See generally Privacy*, NAT'L TELECOMM. & INFO. ADMIN., http://www.ntia.doc.gov/category/privacy (last visited Oct. 5, 2013).

[198] THE WHITE HOUSE, *supra* note 63, at 24.

[199] *Id.* at 27.

more practical than direct regulation, and more effective than self-regulation. At what level should they regulate? They should regulate at the level of the industry sector and not at the level of the firm or of the economy as a whole. The three existing cross-border privacy rule initiatives—the U.S.–E.U. Safe Harbor Agreement, the E.U.'s Binding Corporate Rules program, and the Asian-Pacific Economic Cooperation's Cross-border Privacy Rules initiative—utilize a form of co-regulation, but do so at the level of the firm or of the economy as a whole. This weakens these programs. Governments and industry should experiment with *sector-based co-regulation* as a supplement to the existing initiatives.

Part V showed that it may be possible to implement such a system. E.U. and APEC privacy rules may overlap sufficiently to allow a single code to satisfy both regimes. In addition, the E.U. and APEC systems each include code approval mechanisms that could, with some important modifications, serve as the basis for approving and enforcing sector-based codes that bridge these two regional initiatives. While this solution may be within reach, governments will need to take additional steps to achieve it. This Article further recommends that:

- The E.U. retain Article 27 of the 1995 Data Protection Directive, which allows the Article 29 Working Group to approve sector-based codes and create a legal safe harbor with respect to all E.U. member state data protection laws.[200]
- If the E.U. adopts the General Data Protection Regulation (GDPR), then it should retain Article 38 of the proposed GDPR, which allows the Commission to approve sector-based data protection codes, and so create a legal safe harbor with respect to the GDPR.[201]
- APEC should authorize Accountability Agents to approve *sector-based* codes, not just those that individual companies submit.
- APEC should further define and strengthen the safe harbor that an approved code creates with respect to the national data protection laws of APEC member states. Doing so will increase firms' incentive to participate in the APEC CBPR system.
- If the U.S. Congress passes comprehensive privacy legislation it should include a safe harbor program for industry sectors.[202] This would not only provide a useful, additional tool for U.S. privacy regulation. As set out in this Article, it would also provide a mechanism by which the United States could approve sector-based codes and so, potentially, harmonize its privacy rules with those of the E.U. and the other APEC

---

[200] 1995 Directive, *supra* note 47, art. 27 (explaining how approval of sector-based codes is related to creating a safe harbor).

[201] *Proposed General Regulation*, *supra* note 174, art. 38.

[202] *See, e.g.*, S. 799, 112th Cong. § 501 (2011) (proposing such a safe harbor program); Dennis D. Hirsch & Ira Rubinstein, *Better Safe than Sorry: Designing Effective Safe Harbor Programs for Effective Consumer Privacy Legislation*, 10 Privacy & Security L. Rep. (BNA) 1639 (Nov. 14, 2011) (making specific recommendations on how to design such a safe harbor program).

member states. This is a powerful reason to pass such legislation and to build a safe harbor program into it.

Government adoption of these recommendations would establish a workable system of cross-border privacy rules to govern data flows across all E.U. and APEC member states. Such a system would incorporate the twenty-eight E.U. member nations, as well as the United States, Canada, Japan, China, and other APEC countries. Taken together, these steps would bring us closer to that Holy Grail of contemporary privacy law: unified, clear, protective, and effective international privacy rules.

APPENDIX

Table 3 with Supporting Citations: *Substantive Overlap*

Requirements	E.C. 1995 Directive	E.U. General Regulation	APEC Privacy Principles	U.S. Commercial Privacy Bill of Rights Act
Transparency of Data Practices	✓ [203]	✓ [204]	✓ [205]	✓ [206]
Choice/Consent	✓ [207]	✓ [208]	✓ [209]	✓ [210]
Legitimate Bases (Other than Consent)	✓ [211]	✓ [212]	✓ [213]	✓ [214]
Security Safeguards	✓ [215]	✓ [216]	✓ [217]	✓ [218]
Accuracy	✓ [219]	✓ [220]	✓ [221]	✓ [222]
Access	✓ [223]	✓ [224]	✓ [225]	✓ [226]
Correction	✓ [227]	✓ [228]	✓ [229]	✓ [230]
Purpose Limit on Use	✓ [231]	✓ [232]	✓ [233]	✓ [234]

---

[203] 1995 Directive, *supra* note 47, arts. 10, 18–19, 21.

[204] *Proposed General Regulation*, *supra* note 174, arts. 5(a), 11.

[205] *APEC Framework*, *supra* note 136, paras. 15–17, at 12–13.

[206] S. 799, 112th Cong. § 201(a) (2011).

[207] 1995 Directive, *supra* note 47, arts. 7(a) (consent as general basis for legitimacy), 8(2)(a) ("explicit consent" to processing of sensitive data).

[208] *Proposed General Regulation*, *supra* note 174, art. 6(1)(a).

[209] *APEC Framework*, *supra* note 136, para. 20, at 17.

[210] S. 799 § 202(a)(1)–(3).

[211] 1995 Directive, *supra* note 47, art. 7(b)–(f) (providing legitimate bases for processing other than the data subject's consent to such processing).

[212] *Proposed General Regulation*, *supra* note 174, art. 6(1)(b)–(f).

[213] *APEC Framework*, *supra* note 136, para. 19, at 16–17.

[214] S. 799 § 202(a)(3)(A).

[215] 1995 Directive, *supra* note 47, art. 17 (providing "appropriate technical and organizational measures to protect personal data").

[216] *Proposed General Regulation*, *supra* note 174, art. 30.

[217] *APEC Framework*, *supra* note 136, para. 22, at 21.

[218] S. 799 § 101.

[219] 1995 Directive, *supra* note 47, art. 6(1)(d).

[220] *Proposed General Regulation*, *supra* note 174, art. 5(d).

[221] *APEC Framework*, *supra* note 136, para 21, at 20.

[222] S. 799 § 303.

[223] 1995 Directive, *supra* note 47, art. 12(a).

[224] *Proposed General Regulation*, *supra* note 174, art. 15.

[225] *APEC Framework*, *supra* note 136, paras. 23–25, at 22–24.

[226] S. 799 § 202(a)(4)(A).

[227] 1995 Directive, *supra* note 47, art. 12(b).

[228] *Proposed General Regulation*, *supra* note 174, art. 16.

[229] *APEC Framework*, *supra* note 136, para. 23(c), at 22.

[230] S. 799 § 202(a)(4)(B).

[231] 1995 Directive, *supra* note 47, art. 6(1)(b).

[232] *Proposed General Regulation*, *supra* note 174, art. 5(b).

Requirements	E.C. 1995 Directive	E.U. General Regulation	APEC Privacy Principles	U.S. Commercial Privacy Bill of Rights Act
Sensitive Data	✓ [235]	✓ [236]	(✓) [237]	✓ [238]
Accountability		✓ [239]	✓ [240]	✓ [241]
Purpose Limit on Collection	✓ [242]	✓ [243]	✓ [244]	✓ [245]
Data Minimization	✓ [246]	✓ [247]		✓ [248]
Fair and Lawful	✓ [249]	✓ [250]	✓ [251]	
Retention and Disposal	✓ [252]	✓ [253]		✓ [254]
Privacy by Design		✓ [255]		✓ [256]
Prior Check	✓ [257]	✓ [258]		
Right To Object	✓ [259]	✓ [260]		
Automated Decisions	✓ [261]	✓ [262]		

[233] *See APEC Framework*, *supra* note 136, para. 19, at 16.

[234] S. 799, 112th Cong. §§ 202(b), 302 (2011).

[235] 1995 Directive, *supra* note 47, art. 8(1).

[236] *Proposed General Regulation*, *supra* note 174, art. 9.

[237] By requiring that privacy protections be proportionate to the threatened harm associated with the collection and use of the personal information in question, this provision implicitly differentiates between sensitive personal data (where the threat of harm is great) and other personal information. *See APEC Framework*, *supra* note 136, para. 14, at 11.

[238] S. 799 § 202(a)(3)(A).

[239] *Proposed General Regulation*, *supra* note 174, art. 22.

[240] *APEC Framework*, *supra* note 136, para. 26, at 28.

[241] S. 799 § 102.

[242] 1995 Directive, *supra* note 47, art. 6(1)(b).

[243] *Proposed General Regulation*, *supra* note 174, art. 5(b).

[244] *APEC Framework*, *supra* note 136, para. 18, at 15.

[245] S. 799 § 301(1) (providing that entities shall "collect only as much covered information" as is reasonably necessary to accomplish a list of objectives such as prevent or detect fraud, investigate a possible crime, etc.).

[246] 1995 Directive, *supra* note 47, art. 6(1)(c).

[247] *Proposed General Regulation*, *supra* note 174, art. 5(c).

[248] S. 799 § 301.

[249] 1995 Directive, *supra* note 47, art. 6(1)(a).

[250] *Proposed General Regulation*, *supra* note 174, art. 5(a).

[251] *APEC Framework*, *supra* note 136, para. 18, at 15.

[252] 1995 Directive, *supra* note 47, art. 6(1)(e).

[253] *Proposed General Regulation*, *supra* note 174, art. 5(e).

[254] S. 799 § 301(2).

[255] *Proposed General Regulation*, *supra* note 174, art. 23.

[256] S. 799 § 103.

[257] 1995 Directive, *supra* note 47, art. 20 (requiring that authority conduct prior check of operations "likely to present specific risks" to data subjects).

[258] *Proposed General Regulation*, *supra* note 174, art. 34.

[259] 1995 Directive, *supra* note 47, art. 14 (providing that data subject can object based on "compelling legitimate grounds").

[260] *Proposed General Regulation*, *supra* note 174, art. 19.

Requirements	E.C. 1995 Directive	E.U. General Regulation	APEC Privacy Principles	U.S. Commercial Privacy Bill of Rights Act
Notification to Data Subject	✓ [263]	✓ [264]		
Children's Data Requires Parent's Consent		✓ [265]		(✓) [266]
Data Protection by Default		✓ [267]		
Privacy Impact Assessment		✓ [268]		
Notification to Data Protection Authority	✓ [269]			
Documentation of Processing		✓ [270]		
Right To Be Forgotten and to Erasure		✓ [271]		
Data Portability		✓ [272]		
Preventing Harm			✓ [273]	✓ [274]
Data Protection Officer		✓ [275]		
Supervisory Authority	✓ [276]	✓ [277]		
"Adequacy" Limit for International Transfer	✓ [278]	✓ [279]		

[261] 1995 Directive, *supra* note 47, art. 15 (providing right of data subject not to be subject to decision that significantly affects him and is based on automated data processing).

[262] *Proposed General Regulation*, *supra* note 174, art. 20.

[263] 1995 Directive, *supra* note 47, arts. 10–11.

[264] *Proposed General Regulation*, *supra* note 174, art. 14.

[265] *Id.* art. 8.

[266] This requirement is included in the Children's Online Privacy Protection Act of 1998, which would operate alongside comprehensive policy legislation similar to the Commercial Privacy Bill of Rights Act of 2011 if Congress were to pass such legislation. *See* Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. § 6502(b)(1) (2012).

[267] *Proposed General Regulation*, *supra* note 174, art. 23(2).

[268] *Id.* art. 22(2)(c).

[269] 1995 Directive, *supra* note 47, art. 18.

[270] *Proposed General Regulation*, *supra* note 174, art. 28.

[271] *Id.* art. 17.

[272] *Id.* art. 18.

[273] *APEC Framework*, *supra* note 136, para. 14, at 11 (requiring the privacy protections be designed to prevent harm to individuals, and should be proportionate to the degree of harm threatened by the collection and use of the information in question).

[274] S. 799, 112th Cong. § 202(a)(3)(B)(ii) (2011) (requiring opt-in consent for the use of previously collected information or the transfer of information to a third party for an unauthorized use if the "use or transfer creates a risk of economic or physical harm to an individual").

[275] *Proposed General Regulation*, *supra* note 174, arts. 22(2)(e), 35–37.

[276] 1995 Directive, *supra* note 47, art. 28.

[277] *Proposed General Regulation*, *supra* note 174, art. 46.

[278] 1995 Directive, *supra* note 47, art. 25.

[279] *Proposed General Regulation*, *supra* note 174, art. 41.